REMARKS

This amendment and the following remarks are substantially identical to those presented in the previously un-entered Amendment After Final. With regard to the Examiner's comments in the Advisory Action, Applicant notes that there are numerous features that are absent from Vaeth and Scheidt, as clearly numbered and noted in the remarks regarding those references below. For example, Applicant does not dispute that the term "certificate authority" is used at least once in the Scheidt reference. However, mere recitation of this term does not disclose or suggest the specifically enumerated features described below. Those features are clearly absent from the reference.

This amendment is in response to the Final Office Action dated April 3, 2006. In the amendment, claims 1, 14 and 23 have been amended, and claims 1-36 remain pending in the application. These amendments add no new matter. Reconsideration of the pending claims is respectfully requested.

Claims 13, 22 and 35 have been rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim what Applicant regards as the invention. This rejection is traversed.

The Examiner objects to language in the noted dependent claims stating the "each of said plurality of signature modules respectively executes multiple signature algorithms" whereas the corresponding independent claims recite "a plurality of signature modules each executing a different signature algorithm."

Applicant appreciates the Examiner's attention to the claims. However, Applicant notes that the above-mentioned features are not mutually exclusive. A signature module can satisfy the requirement of executing a different signature algorithm from other signatures modules, while still executing multiple signature algorithms. As a simple example, presume that signature module #1 executes signature algorithms A&B and signature module #2 executes signature algorithms C&D (or even B&C). Each signature module would execute a different signature algorithm (*e.g.*, A and C), yet still execute multiple signature algorithms.

Applicant also notes that dependent claims 13, 22 and 35 do not "broaden" the respective independent claims. Rather, they actually narrow the independent claims in that they require the signature modules to execute multiple signature algorithms, whereas the independent claims do

not.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 13, 22 and 35 as being indefinite under 35 U.S.C. § 112, second paragraph.

Claims 1-3, 5, 6, 8-12, 14-21, 23-25, 27, 28, 30-34 and 36 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 5,659,616 to Sudia ("Sudia") in view of U.S. Pat. No. 6,035,402 to Vaeth et al. ("Vaeth"), and further in view of U.S. Pat. No. 6,490,680 to Scheidt et al. ("Scheidt"). This rejection is traversed.

Claim 1 recites: *[a] public key certificate issuing system comprising:*

a certificate authority for issuing a public key certificate used by an entity; and

a registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority;

wherein said certificate authority, having a plurality of signature modules each executing a different signature algorithm, selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned signature algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned signature algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.

With these claimed features, a registration authority receives a public key certificate request and transmits the request to the certificate authority. The certificate authority has a plurality of signature modules each executing a different signature algorithm. The certification authority uses a table that associates the registration authority that has made the request to an assigned signature algorithm. The selection of a particular signature module (and corresponding signature algorithm) is thus made with reference to this table, which identifies the assigned signature algorithm.

These claimed features are not disclosed or suggested by Sudia, Vaeth and Scheidt, whether taken individually or in any combination.

Sudia discloses a cryptographic system that encodes security policy and authorization information into signatures and certificates by employing attribute certificates. (Sudia, Abstract). As admitted by the Examiner, Sudia does not disclose (and indeed offers no mention of) a registration authority. (Office Action, p. 5). Since Sudia does not even generally disclose a registration authority, the reference cannot properly be construed to disclose (1) transmission of a received request from a registration authority to a certificate authority, (2) referencing a table that that associates the registration authority with an assigned signature algorithm; or (3) selecting one of the plurality of signature modules based upon the identification of the assigned signature algorithm.

Vaeth and Scheidt do not remedy the deficiencies of Sudia. Vaeth discloses a system wherein requests for a certificate are directed to a certificate authority, where they are held and accessed by a registration authority that is said to have verification responsibilities. (Vaeth, Abstract). The registration authority is also referred to as a "virtual" certificate authority in that information required on a certification request data form may be determined by the registration authority, although the form is held at and distributed from the certificate authority. (Vaeth, at 8:3-6). Vaeth uses the term "registration authority", but that entity does not appear to participate in the authentication process in the fashion claimed by Applicant. Thus, it is not clear that Vaeth even offers a disclosure of the first feature noted as being absent from Sudia, namely the transmission of a received request from the registration authority to the certificate authority.

Nevertheless, even assuming that Vaeth discloses such a feature, the reference most certainly offers no disclosure or suggestion of (2) referencing a table that that associates the registration authority with an assigned signature algorithm; or (3) selecting one of the plurality of signature modules based upon the identification of the assigned signature algorithm. At best, Vaeth discloses some type of system wherein a "certificate authority" and a "registration authority" participate. There is no selection of a signature module based upon an identification of an assigned signature algorithm, or of referencing a table associating the requesting registration authority to the assigned signature algorithm in order to make that selection.

Scheidt, the third reference relied upon by the Examiner, discloses an access control and authorization system. The system, referred to as a Constructive Key Management System, or "CKM", is said to include a Policy Manager as a first tier and a Credential Manager as a second tier. The Policy Manager serves as the central authority and generates encryption keys and

manages encryption algorithms. (Scheidt, at 7:44-58). The Credential Manager is alleged, by the Examiner, to disclose the certificate authority of Applicant's claimed invention. As understood by Applicant, the Credential Manager "accepts as input, subsets of encryption algorithms, organizational policies, and system parameters, which are managed by the Policy Manager." (Scheidt, at 7:62-65). It is unclear how the Credential Manager of Scheidt relates to a certificate authority as claimed by Applicant. The Examiner makes reference to a database, which apparently is the User Credentials database. At best, the Credential Manager performs some type of management of user credentials. There are no details whatsoever of receiving requests from registration authorities, or of correlating particular registration authorities to assigned signature algorithms, or selecting signature modules based upon identification of an assigned signature algorithm. Thus, Scheidt clearly fails to disclose or suggest (1) transmission of a received request from a registration authority to a certificate authority, (2) referencing a table that that associates the registration authority with an assigned signature algorithm; or (3) selecting one of the plurality of signature modules based upon the identification of the assigned signature algorithm.

Independent claims 14, 23, and 36 are also neither disclosed nor suggested by Sudia, Vaeth, or Scheidt for reasons similar to those provided regarding claim 1 above.

Since even the combination of Sudia, Vaeth and Scheidt would still fail to disclose features that are recited in Applicant's independent claims, Applicant submits that the Examiner has failed to produce a prima facie case of obviousness. Applicant also reiterates that, even if the combination would produce the claimed features, which is not the case, such a combination would be improper as there is no motivation to combine the references in the fashion offered by the Examiner. Common subject matter and classification are not dispositive of this issue. Simply, there is no clear explanation as to how these references would be combined in some logical fashion.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of the noted independent claims as being unpatentable over the combination of Sudia, Vaeth and Scheidt, as well as the corresponding dependent claims that incorporate the described features and that respectively add their own distinct features.

Claims 4, 7, 26 and 29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Sudia, Vaeth, and Scheidt, and further in view of U.S. Pat. No. 6,202,157 to Brownlie et al. ("Brownlie"). This rejection is traversed.

Claims 4, 7, 26 and 29 depend either directly or indirectly from the above-described independent claims and thus incorporate the features contained therein. Brownlie discloses a computer network security system. As with the first three relied-upon references, there is no apparent disclosure or suggestion in Brownlie of (1) transmission of a received request from a registration authority to a certificate authority, (2) referencing a table that that associates the registration authority with an assigned signature algorithm; or (3) selecting one of the plurality of signature modules based upon the identification of the assigned signature algorithm. Thus, the proposed combination would still fail to yield the features incorporated into these dependent claims, let alone the additional features separately recited therein.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 4, 7, 26 and 29 under 35 U.S.C. § 103(a).

Claims 13, 22 and 35 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Sudia, Vaeth, and Scheidt, and further in view of U.S. Pat. No. 6,675,296 to Boeyen et al. ("Boeyen"). This rejection is traversed.

Boeyen discloses certificate format conversion. There is no mention, even generally, of a registration authority or a relationship between a registration authority and certificate authority as claimed by Applicant. Thus, there is once again no disclosure or suggestion of (1) transmission of a received request from a registration authority to a certificate authority, (2) referencing a table that that associates the registration authority with an assigned signature algorithm; or (3) selecting one of the plurality of signature modules based upon the identification of the assigned signature algorithm, so the proposed combination would still fail to yield the features incorporated into these dependent claims, let alone the additional features separately recited therein.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 13, 22 and 35 under 35 U.S.C. § 103(a).

For the foregoing reasons, reconsideration and allowance of the claims which remain in this application are solicited. If any further issues remain, the Examiner is invited to telephone the undersigned to resolve them.

Dated: June 20, 2006

Respectfully submitted,

By _____ 40,290

Ronald P. Kananen
Registration No. 24,104
Christopher M. Tobin
Registration No.: 40,290
RADER, FISHMAN & GRAUER PLLC
1233 20th Street, N.W., Suite 501
Washington, DC 20036
(202) 955-3750
Attorney for Applicant